AT-S94 Version 3.0.0.41
AT-8000S Switch
Software Release Notes

Please read this document before you begin to use the management software.

Caution
Failure to upgrade the bootloader before the release software can result in a switch that will not boot. Please read the upgrade instructions in this SRN carefully.

This document contains the following sections:

- "Supported Platforms" on page 2
- "Product Documentation and Software" on page 2
- "What's New in Version 3.0.0.41" on page 3
  - "New Software Features" on page 3
  - "Resolved Issues" on page 3
  - "Operational Notes" on page 3
  - "Known Issues" on page 4
  - "New Hardware Features" on page 4
- "Version 3.0.0.41 Upgrade Process" on page 5
  - "Software Installed with Incorrect Bootloader" on page 7
- "History of Resolved Issues" on page 8
- "Features History" on page 9
- "Upgrade Procedure from Version 1.0.0.25" on page 12
- "Contacting Allied Telesis" on page 16

Supported Platforms

The following platforms are included in the AT-8000S family of devices:

- AT-8000S/16 – 16 FE ports with 1 combo 10/100/1000 SFP Port.
- AT-8000S/24 – 24 FE ports with modular configuration 2 x combo 10/100/1000 SFP ports and 2 RJ-45 10/100/1000 stacking ports.
- AT-8000S/24POE – 24 FE ports with modular configuration 2 x combo 10/100/1000 SFP ports and
  2 RJ-45 10/100/1000 stacking ports, with support for Power over Ethernet on all ports.
- AT-8000S/48 – 48 FE ports with modular configuration 2 x combo 10/100/1000 SFP ports and 2 RJ-45 10/100/1000 stacking ports.
- AT-8000S/48POE – 48 FE ports with modular configuration 2 x combo 10/100/1000 SFP ports and
  2 RJ-45 10/100/1000 stacking ports, with support for Power over Ethernet on up to 36 ports.

The AT-8000S/24, AT-8000S/24POE, AT-8000S/48 and AT-8000S/48POE can be combined together in a six-unit high stack.

Product Documentation and Software

For description how to install the devices as standalone units or as members of a stack, refer to the following guide:

- AT-8000S Installation Guide

For lists of CLI commands available to the user to configure the devices, refer to the following guide:

- AT-8000S CLI Reference Guide

See “Management Software Updates” on page 16 for instructions for accessing these documents.

What's New in Version 3.0.0.41

New Software Features

- None

Resolved Issues

- In some cases where more than one switch has the same STP Bridge Priority value in a network, the switch with the higher MAC address would be elected as the STP root bridge. This issue has been resolved.

Operational Notes

- **100 Mbps SFP:** Switch over back to fiber fails after fiber link restored. It happens when an LCP155A4HSR 100M SFP is used when backup Copper link is 1G.
  Recommended User Work Around: Works fine when fiber and Copper speeds are similar and there are no issues with different SFP model.
- **Port Mirroring:** Port mirroring closes the port and opens it again.
  Recommended User Work Around: Not required.
- **TAB functionality:** Use of the Tab key does not complete the command Interface range VLAN all and the command Switchport general allowed VLAN.
  Recommended User Work Around: Type in the full command.
- **SNMP - EWS > SNMP > Notify > Filters:** Cannot add or modify filter with name containing special characters.
  Recommended User Work Around: Do not use special characters.
- **Time - EWS > System > System Time:** The current day becomes undefined after changing Time Zone Offset.
  Recommended User Work Around: The current day will be displayed correctly when the switch is reset.
- **Web Response Time:** Upon full table configuration it takes longer time to open the page IPv6 Neighbors and the page Statistics->RMON Alarm.
- **Flow Control:** Flow control does not work on the Gigabit ports.
  Recommended User Work Around: No work around.
- **Encryption:** It is impossible to add MD5/SHA keys via EWS.
  Recommended User Work Around: Use CLI commands.
- **Syslog:** Fail to add one syslog server with a description of maximum length including some space.
  Recommended User Work Around: Do not use spaces and avoid using the maximum allows length of the description.
- **LLDP:** When in mixed stack of PoE and Non PoE units, you can configure the PoE-PSE optional TLVs for non-PoE ports and these non-PoE ports will be advertised.
  Recommended User Work Around: Do not configure the PoE-PSE optional TLVs for non-PoE ports, so that this information will not be advertised.
- **TACACS:** When using the single connection option, the first login or "enable" attempts will fail, but the retry works.
  Recommended User Work Around: Use the multiple connection option (default setting).

- **Port lock:** Port security mechanism is not triggered for MAC violation if MAC is learned on another locked port as a secured MAC address.
  Recommended User Work Around: No work around
- **Mac-group mapping and 802.1x:** Mac-group mapping on the same port on which 802.1x takes place, stops the authentication.
  Recommended User Work Around: Use DVA instead.
- **IGMP snooping and private VLAN:** IGMP snooping and private VLAN will not work on the same port. **Recommended User Work Around:** No work around.
- **Mac authentication:** MAC authorization fails if the default of the radius server is not md5.
  Recommended User Work Around: Use md5 as default of the radius server.

Known Issues

- None

New Hardware Features

- None

Version 3.0.0.41 Upgrade Process

You must have the correct software and bootloader installed on your switch before beginning the upgrade process to Version 3.0.0.41. Perform the following procedure:

Note
If you have a stacked configuration, all switches must be running the latest bootloader and the same software version before you upgrade the software for the stack.

Note
You can download Version 3.0.0.41 files from our web site at **www.alliedtelesis.com**. Refer to “Management Software Updates” on page 16 for instructions on how to navigate to the software updates page for the AT-8000S. All of the file names referenced below are contained in the zip file that you download.

1. Log into the switch.
2. For a successful software upgrade of your AT-8000S switch, it is mandatory that you first install the latest boot loader file (s94bv10107.rfb). You can find this file in the Latest_Boot_Loader folder that you have downloaded from the Allied Telesis web site.
3. Verify that your switches are running the correct boot loader and management software by using the following command:

   ```
   show version
   ```

4. If your AT-8000S series switch has Version 1.0.0.25 (or earlier) currently installed on it, go to the “Upgrade Procedure from Version 1.0.0.25” on page 12. and follow the steps to upgrade to Version 3.0.0.41. If your AT-8000S series switch has Version 1.1.0.32 or later installed on it, go to the next step to upgrade to Version 3.0.0.41.
5. With information displayed from the “show version” command, copy the boot version number exactly as shown. Using this number as the password, extract the ats94-30041.ros software upgrade file from the ats94-30041.zip file.

6. Assuming your switch is running the correct bootloader, you have the correct password to extract the ats94-30041.ros software upgrade file and you know that your current bootloader is compatible with the Version 3.0.0.41 software. If this is the case, you can proceed with the version 3.0.0.41 software upgrade by following steps 9 - 11. If this is not the case,

7. If your switch is NOT running the correct bootloader version and you can NOT extract the ats94-30041.ros software upgrade file and you must install the latest boot loader file provided (s94bv10107.rfb) by using the following commands:

   Note
   You must substitute the IP address of your local TFTP server.

   For a stand alone switch -

   ```
   Copy tftp://192.168.1.10/s94bv10107.rfb boot
   ```

   For a stack configuration -

   ```
   Copy tftp://192.168.1.10/s94bv10107.rfb unit://*/boot
   ```

8. Verify that your switches are running the correct boot loader by using the following command:

   ```
   show version
   ```

   With information displayed from the “show version” command, copy the boot version number exactly as shown. Using this number as the password, extract the ats94-30041.ros software upgrade file from the ats94-30041.zip file.

9. Use one of the following commands depending on your configuration:

   Note
   You must substitute the IP address of your local TFTP server.

   For a stand alone switch -

   ```
   Copy tftp://192.168.1.10/ats94-30041.ros image
   ```

   For a stack configuration -

   ```
   Copy tftp://192.168.1.10/ats94-30041.ros unit://*/image
   ```

10. Before rebooting the stand alone switch or stack, you must change the active image, including each slave switch in the stack. To check the active image for each switch use the following command.

    ```
    Show bootvar
    ```

    The resulting display will tell you which image is active on each switch. Depending on your configuration, you can now issue one of the following commands, substituting x and y from the Show bootvar command:
    For a stand alone switch -

    ```
    Boot sys image-y
    ```

    For each switch in a stack -

    ```
    Boot sys unit x image-y
    ```

    Switch the active image for next reboot.

11. Reboot the device with the command:

    ```
    reload
    ```

    This command will cause the switch to reboot. By the end of the reboot process, Version 3.0.0.41 software will be running.

Software Installed with Incorrect Bootloader

If you accidentally install the version 3.0.0.41 software on a switch without the latest boot loader, the switch will fail to boot properly. To recover from this situation, you must obtain a previous version of software (V3.0.0.35 or V3.0.0.38) from our ATI web site and perform the following procedure to install this software using the XMODEM protocol:

1. Set up a console port connection.
2. Power cycle the switch.
3. Quickly press the Enter key when the switch displays the following line:

   Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.

4. If you hit the Enter key quickly enough, the following Menu is displayed:

   Startup Menu
   [1] Download Software
   [2] Erase Flash File
   [3] Enter Diagnostic Mode
   [4] Set Terminal Baud-Rate
   [5] Back
   Enter your choice or press 'ESC' to exit:

5. Select number one by pressing the ‘1’ key.
   The switch will respond with the following message:

   Begin the transmission of a previous version.
   Downloading code using XMODEM.
   You may proceed with the xmodem transfer.

6. When the download is complete, reboot the switch.

7. Install the latest boot loader (s94bv10107.rfb) using the *copy* command. You may use the xmodem or TFTP options as described in the AT-8000S CLI Reference Guide.

8. Install the Version 3.0.0.41 software by the following steps 6 - 8 in “Upgrade Procedure from Version 1.0.0.25” on page 12.

History of Resolved Issues

Version 3.0.0.40

- PC is beginning re-authentication after 30 seconds and this fails although still have connectivity. (CQ 117489 ATI 188)
- NAP is not working. (CQ 117116 ATI 199)
- Operation MAU in LLDP_MAD MAC/PHY TLV is 0 instead of 16. (CQ 117561 ATI 208)
- Does not learn more than 30 LLDP-MED end points (CQ 121240 ATI 235)
- Problem with IGMP Snooping on AT-8000S/48 stack - fatal error. (CQ 121102 ATI 230)
- GVRP + LACP - GVRP does not recover after a fail. (CQ 120476 ATI 234)
- Problem with IGMP Snooping on AT-8000S/48 stack - fatal error operation - SW2M: ABORT DATA exception. (CQ 122604)
- Stack issue - broadcast blocked when using “bridge multicast unregistered filtering”. (CQ 122469 ATI 244, ATI 251)

Version 3.0.0.38

- udp-mib - definition for udpHCGroup has been commented out. (CQ ID 119274)
- The rlpoe.mib has an incorrect module name. (CQ 118708 ATI 221)
- DHCP snooping doesn't work on guest VLAN. (CQ 117217 ATI 204)
- The command “default-vlan vlan” is not available on 8000S. (CQ 118706 ATI 219)
- Cannot apply IP ACL because of lack of HW resources. (CQ 118117 ATI 214)
- There is no support for MIB counters ifInErrors & ifOutErrors.(CQ 117172 ATI 202)

Version 3.0.0.35

- Multicast - When several multicast groups are registered on a port, all will be deleted when an IGMP Leave report for just 1 of the groups is received on the port (CQ ID114173)
- EWS - User can not add a VLAN via GUI interface if the VLAN ID starts with 5,6,7,8,9 (CQ ID 115354)
- SNMP - Added support for SNMP trap when master stack unit is down (CQ ID 117040)

Version 3.0.0.33

- When the master was lost (powered down) the SFP port(s) on backup changed to DOWN – link changed to half duplex and remained down. This issue has been resolved.

Version 3.0.0.32

- Unregistered Multicast - when a user configures unregistered multicast to be filtered then broadcast packets were mistakenly also identified as unregistered multicast and therefore were also filtered (CQ ID 112258)
- DVA - When the bridge address table is full and unregistered multicast are set to be filtered the device fails with fatal error (CQ ID 112338)
- The MAC groups mapping is not working for IGMP packets (CQ ID 89459)
- Guest VLAN should be accessible only after timeout/fail authentication (CQ ID 68048)
- Dynamic VLAN assignment need to allow support for tag<>0 in attribute [81] Tunnel-Private-Group-Id (CQ ID 103461)
- Command qos wrr-queue threshold should be removed from the CLI Guide (CQ ID 104433)
- Traffic shaping should not be applied if port is in half duplex (CQ ID 106326)
- FE/GE ports, Storm control range of supported values is incorrect in the CLI guide (CQ ID 108733)
- In order to get a clean, functional compile using Castlerock SNMP need to make a few changes to the MIB files (CQ ID 109360)
- SYSLOG - on EWS system/event log modify tab “minimum severity” should be changed to”facility” (CQ ID 111154)
- SNMPv1/2 - MIB file: Some mib files compile error (CQ ID 111073)
- SNTP - After enabling SNTP via EWS, the SNTP Unicast Clients and Unicast Clients polling is still not enabled (CQ ID 110764)
- EWS - At standalone DUT, EWS will display non-existed port g3,g4 (CQ ID 110769)
- Diagnostic LED - The Diagnostic LED Indications in Table 7 on Page 20 of the AT-8000S Installation Guide should read as follows:

LED Description	LED Indication	Description
Diag	Green	System Diagnostics in progress.
	Off	System Diagnostics successfully completed.

Features History

Version 3.0.0.40

- **Dot1x Legacy compliant**

This is an advanced 802.1x configuration enabling support for non-compliant 802.1x devices such as Windows XP SP2.

- The following is a new CLI command introduced in Version 3.0.0.40:

Table 1: CLI Command

CLI Command	Description of Functionality
dot1x legacy-supp-mode	Use the dot1x legacy-supp-mode interface configuration command in multiple session mode to enable 802.1x switch to send periodic EAPOL request identity frame according to tx timeout period. This is the default behavior

Version 3.0.0.38

- No new features were introduced in this release.

Version 3.0.0.35

- No new features were introduced in this release.

Version 3.0.0.33

- No new features were introduced in this release.

Version 3.0.0.32

- **Dynamic VLAN Assignment (DVA)** - The system supports Dynamic VLAN assignment based on 802.1x RADIUS Attributes. A predefined VLAN is assigned to a new user/port, after successful authentication of that user/port.
- **Forwarding/Filtering of Unregistered Multicast Frames** - This feature enables to configure how to handle MC Frames that belong to unregistered MC groups.

Unregistered MC groups are the groups that are not known to the switch. The switch learns about MC groups by IGMP Snooping, or by static configuration.

Normally, MC frames are always flooded to all ports in the VLAN. If IGMP Snooping is enabled, the switch learns about existence of MC groups and keeps track of which ports have joined to which MC group. This enables the switch to forward the MC frames (from a registered MC group) only to ports that are registered to that MC group. All unregistered MC frames, i.e., the MC frames that do not belong to a registered MC group, are still flooded to all ports on the VLAN.

The “Forwarding/Filtering of Unregistered MC Frames” feature enables to configure whether to forward or to filter these MC frames.

- **STP BPDU Guard** - BPDU Guard is used as a security mechanism to protect the network from invalid configurations.

BPDU Guard is usually used either when fast link ports (ports connected to clients) are enabled or when STP feature is disabled. When BPDU guard is enabled on a port, the port is shut down if a BPDU message is received and an appropriate SNMP trap is generated.

- **RADIUS Accounting** - The feature enables to record device management sessions (Telnet, serial and WEB but not SNMP) and or 802.1x authentication sessions.
- **802.1x Enhanced Features** - This release supports 802.1x Multi Session mode enabling multiple 802.1x sessions simultaneously on a port. This allows number of specific hosts that have been authorized to get access to the port. Filtering is based on the source MAC addresses.

The following 802.1x feature enhancements will be supported:

— Guest VLAN - This feature allows network administrators to give some limited access to the network to unauthorized ports. The port would be a member in the Guest VLAN only after specific timeout from “port up” (letting the supplicant to start the 802.1x), or after 802.1x authentication failure

— Unauthenticated VLAN - This feature allows network administrators to define VLANs when authorization is not required for them.

❒ **802.1ab LLDP**

— LLDP - 802.1ab is an IEEE standard for Link Layer Discovery Protocol in Ethernet networks. It provides a method for switches, routers and access points to advertise their identification, configuration and capabilities to neighboring devices that store the data in a MIB (management information base). Link layer discovery allows a network management system to model the topology of the network by interrogating the MIB databases in the devices.

— LLDP-MED - The Link Layer Discovery Protocol – Media Endpoint is an extension of the 802.1ab IEEE standard of LLDP providing behavioral requirements for devices implementing the extensions to enable correct multi-vendor interoperation.

❒ **IPv6 Host** - The device functions as an IPv6 compliant Host, as well as IPv4 Host. This functionality is provided in a pure IPv6 network as well as in a combined IPv4/IPv6 network.

Note
IPv6 was not tested for UNH/DoD certification.

❒ **Configurable Login Banner** - The system supports a text based banner that is configurable via CLI Command to enable telnet session to display security messages above the login prompt prior to login.

Upgrade Procedure from Version 1.0.0.25

All software released after version 1.0.0.25 requires additional FLASH sectors beyond the current amount of FLASH sectors currently allocated for the image. Therefore the FLASH sectors must be reordered before downloading the new software. This will be accomplished by first downloading an interim version, and only after that loading the actual released version.

Note
Due to new Board Support Package (BSP) there is also an updated Boot code: version 1.0.0.7. This can be uploaded regardless of the SW image (ROS version) running on the device. Therefore, boot upgrade can be performed before or after the upgrade procedure described below

The interim version provided reorders the FLASH allocation without the need to erase the FLASH and downloading the new software via the serial cable using XMODEM. Hence, the AT-8000S software upgrade procedure can be performed via TFTP server. The block diagram of this procedure is shown in Figure 1.

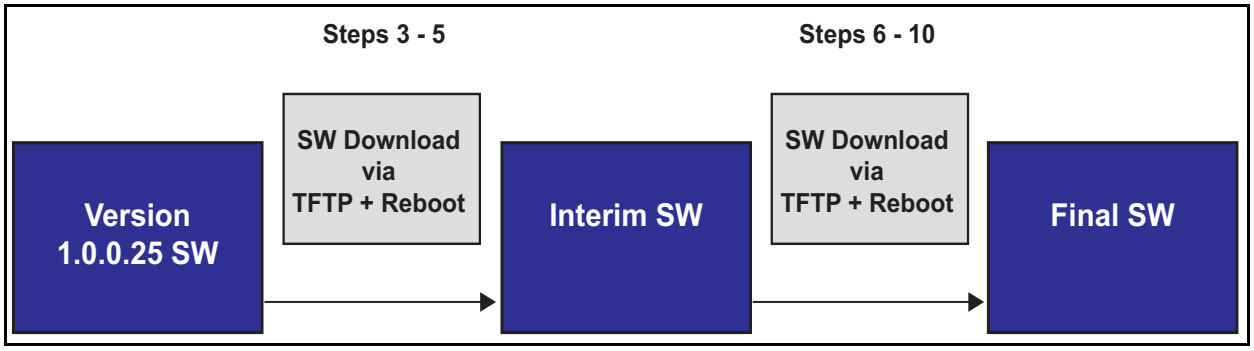

Figure 1. Software Upgrade Process from Version 1.0.0.25

The existing configuration is retained including MAC address and serial number.

Note
During the software upgrade ensure the following:

- Ensure that the device is not powered down or that a power cable is not disconnected during the software upgrade. If the device is powered down or if a cable is disconnected, once device is reconnected the software upgrade must be downloaded via XMODEM
- Ensure that the device configuration is backed up to an external server/station.
- Do not use the interim code drop for Quality Assurance testing, field upgrades etc; use only the final code drop
- When running the interim version, the initialization stage takes a relatively long time

The user will have to run the following steps in order to successfully completing the upgrade procedure:

1. Back up configuration files to an external device.

2. Download the ats94-Interim image drop to the device via TFTP by using one of the following commands depending on your configuration:

   Note
   You must substitute the IP address of your local TFTP server.

   For a stand alone switch -

   ```
   Copy tftp://192.168.1.10/ats94-interim.ros image
   ```

   For a stack configuration -

   ```
   Copy tftp://192.168.1.10/ats94-interim.ros unit://*/image
   ```

3. Before rebooting the stand alone switch or stack, you must change the active image, including each slave switch in the stack. To check the active image for each switch use the following command.

   ```
   Show bootvar
   ```

   The resulting display will tell you which image is active on each switch. Depending on your configuration, you can now issue one of the following commands, substituting x and y from the Show bootvar command:
   For a stand alone switch -

   ```
   Boot sys image-y
   ```

   For each switch in a stack -

   ```
   Boot sys unit x image-y
   ```

   Switch the active image for next reboot.

4. Reboot the device. By the end of the reboot process (which may take a few minutes), the interim code drop version will be running on the device, and it will automatically rearrange the FLASH sectors as needed.

5. Obtain the Version 3.0.0.38 software from out ATI web site. See “Management Software Updates” on page 16 to navigate to this file.

6. Download the Version 3.0.0.38 software via TFTP by using one of the following commands depending on your configuration:

   For a stand alone switch -

   ```
   Copy tftp://192.168.1.10/ats94-30038.ros image
   ```

   For a stack configuration -

   ```
   Copy tftp://192.168.1.10/ats94-30038.ros unit://*/image
   ```

7. Before rebooting the stand alone switch or stack, you must change the active image, including each slave switch in the stack. To check the active image for each switch use the following command.

   ```
   Show bootvar
   ```

8. The resulting display will tell you which image is active on each switch. Depending on your configuration, you can now issue one of the following commands, substituting x and y from the Show bootvar command:

   For a stand alone switch -

   ```
   Boot sys image-y
   ```

   For each switch in a stack -

   ```
   Boot sys unit x image-y
   ```

9. This command will switch the active image for next reboot.

10. Download the latest boot loader file (s94bv10107.rfb) to your switch or stack. You can find this file in the Latest_Boot_Loader folder that you have downloaded from the Allied Telesis web site. Use one of the following commands depending on your configuration:

    Note
    You must substitute the IP address of your local TFTP server.

    For a stand alone switch -

    ```
    Copy tftp://192.168.1.10/s94bv10107.rfb boot
    ```

    For a stack configuration -

    ```
    Copy tftp://192.168.1.10/s94bv10107.rfb unit://*/boot
    ```

11. Verify that your switches are running the correct boot loader and management software by using the following command:

    ```
    show version
    ```

12. Assuming your switch is running the correct bootloader, you have the correct password to extract the ats94-30041.ros software upgrade file and you know that your current bootloader is compatible with the Version 3.0.0.41 software.

13. Download the Version 3.0.0.41 software via TFTP by using one of the following commands depending on your configuration:

    For a stand alone switch -

    ```
    Copy tftp://192.168.1.10/ats94-30041.ros image
    ```

    For a stack configuration -

    ```
    Copy tftp://192.168.1.10/ats94-30041.ros unit://*/image
    ```

14. Before rebooting the stand alone switch or stack, you must change the active image, including each slave switch in the stack. To check the active image for each switch use the following command.

    ```
    Show bootvar
    ```

15. The resulting display will tell you which image is active on each switch. Depending on your configuration, you can now issue one of the following commands, substituting x and y from the Show bootvar command:

    For a stand alone switch -

    ```
    Boot sys image-y
    ```

    For each switch in a stack -

    ```
    Boot sys unit x image-y
    ```

    This command will switch the active image for next reboot.

16. Reboot the device with the command:

    ```
    reload
    ```

    This command will cause the switch to reboot. By the end of the reboot process, the final code drop will be running.

17. Download saved configuration (if needed) to the device.

Note
In case of a stack both the interim version and the final version should be downloaded to ALL the units in the stack at the same time

Note
Following this procedure and uploading the interim code drop is required only once. Any future S/W upgrades will not require the additional upload of the interim code drop.

Contacting Allied Telesis

This section provides Allied Telesis contact information for technical support as well as sales and corporate information.

Online Support

You can request technical support online by accessing the Allied Telesis Knowledge Base: **www.alliedtelesis.com/support**. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support & Services section of the Allied Telesis web site: **www.alliedtelesis.com/support**. Select your country from the list displayed on the website. then select the appropriate menu tab.

Warranty

For hardware warranty information, refer to the Allied Telesis web site: **www.alliedtelesis.com/support**.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesis without an RMA number will be returned to the sender at the sender's expense. To obtain an RMA number, contact the Allied Telesis Technical Support group at our web site: **www.alliedtelesis.com/support**. Select your country from the list displayed on the website. Then select the appropriate menu tab.

Sales or Corporate Information

You can contact Allied Telesis for sales or corporate information through our web site: **www.alliedtelesis.com**. To find the contact information for your country, select Contact Us.

Management Software Updates

New releases of management software for our managed products are available on our Allied Telesis web site at **http://www.alliedtelesis.com/support**.

Copyright © 2011 Allied Telesis, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis and the Allied Telesis logo are trademarks of Allied Telesis, Incorporated. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice.